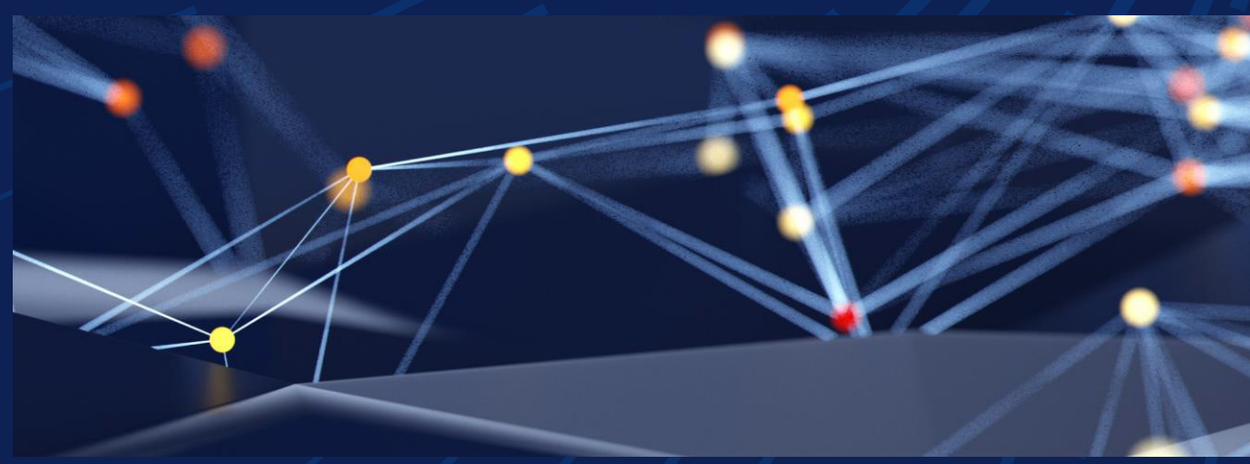
De toekomst van cyberbeveiliging:

Aanpassen aan een nieuw digitaal tijdperk



Hoewel cyberbeveiligingsprofessionals zich vaak richten op het voorkomen van aanvallen en het opstellen van herstelplannen zijn, is de algehele beveiligingsomgeving voortdurend in beweging. Het is daarom belangrijk om vooruit te plannen voor wat er komen gaat.

Als we naar de toekomst kijken, springen drie gebieden eruit: post-kwantumcryptografie, de veranderende regelgeving en opkomende bedreigingen. Organisaties moeten nu actie ondernemen door oplossingen in te plannen en te implementeren zodra deze beschikbaar zijn.

De opkomst van post-kwantumcryptografie

Kwantumcomputing belooft industrieën te transformeren, omdat het verbazingwekkende rekenkracht biedt waarmee problemen kunnen worden opgelost die ver buiten het bereik van klassieke computers liggen. Deze zelfde kracht zou de huidige cryptografische methoden echter overbodig kunnen maken. Algoritmen zoals RSA en ECC, die de basis vormen voor veel van de huidige beveiligde communicatie, kunnen binnen enkele seconden gekraakt worden door een geavanceerde kwantumcomputer. Door deze dreiging is de behoefte aan post-kwantumcryptografie toegenomen.

Post-kwantumcryptografie (PQC) draait om het ontwikkelen van cryptografische algoritmen die beveiligd blijven in een tijdperk van kwantumcomputers. Het National Institute of Standards and Technology (NIST) onderkent dit dreigende risico en neemt het voortouw bij het standaardiseren van kwantumbestendige algoritmen.

Voor bedrijven is de voorbereiding op deze overgang onontkoombaar. Vroegtijdige implementatie van PQC-oplossingen zorgt ervoor dat data beveiligd blijven wanneer kwaadwillenden toegang krijgen tot kwantumcomputing.

Zoals Bobbie Stempfley, VP Cybersecurity en een Business Unit Security Officer bij Dell aangeeft, moeten organisaties het proces beginnen door zich te richten op twee belangrijke gebieden:

Alle cryptografische modellen identificeren en inventariseren die momenteel in gebruik zijn

Houd ook rekening met actieve data, niet alleen met inactieve data. Denk aan sleutelbeheer, codeondertekening, apparaatidentificaties, beveiligde toegang en telemetrie. Maak een uitgebreide inventarisatie en stel vervolgens een roadmap op.

De status van leveranciers onderzoeken

Aangezien moderne ondernemingen soms wel duizenden leveranciers hebben, moet u zich bewust zijn van de risico's die hieruit kunnen voortvloeien. Zorg ervoor dat zij ook plannen maken om mee te veranderen.

Voer naast deze uitgangspunten risicobeoordelingen uit om kwetsbare systemen te identificeren, overweeg hybride cryptografische modellen te implementeren om operationeel te blijven tijdens de overgang en werk samen met leveranciers die al werken met kwantumveilige oplossingen. Houd er wel rekening mee dat niet één leverancier of technologie een kant-en-klare oplossing biedt.

Veranderingen in regelgeving in een geglobaliseerde wereld

Een andere belangrijke factor voor de toekomst van cyberbeveiliging is de veranderende regelgeving. Regelgeving gaat nu veel verder dan naleving; het wordt een belangrijk framework voor het afleggen van verantwoording, het stimuleren van technologische upgrades en het beschermen van burgers in een onderling verbonden, datagestuurde wereld. Regels evolueren echter snel en variëren aanzienlijk per regio, waardoor de complexiteit van naleving toeneemt.

Toch gaan deze verder dan alleen sancties als u deze niet naleeft; ze dienen als katalysator voor betere methoden van cyberbeveiliging. Bedrijven die hun beleid actief afstemmen op wettelijke vereisten, kunnen een nieuw niveau van vertrouwen en operationele efficiëntie bereiken. Hiervoor moeten organisaties governanceframeworks opstellen waarmee ze flexibel blijven om aan wettelijke wijzigingen te blijven voldoen, regelmatige nalevingscontroles uitvoeren en investeren in training van werknemers om gevoelige informatie te verwerken in overeenstemming met de nieuwste normen.

Nu beveiligingsmanagers zich voorbereiden op naleving, is het belangrijk dat ze ervoor zorgen dat ze duidelijk taalgebruik hanteren. Maar al te vaak gebruiken beveiligingsprofessionals beveiligingstermen die misschien niet overkomen bij klanten, regelgevers en andere belanghebbenden. Het is aan de beveiligingsprofessionals om ervoor te zorgen dat ze worden begrepen, niet aan de luisteraars om alles te interpreteren.

> Zie de verschuiving naar post-kwantumcryptografie als het optillen en verplaatsen van een volledig gemeubileerd huis. Zo complex zal het zijn, en de uitdaging is om daarbij niets kapot te maken."
>
> ***Bobbie Stempfley***
> *VP, Cybersecurity en Business Unit Security Officer, Dell Technologies*

De evolutie van het dreigings- (en verdedigings-)landschap

AI brengt een revolutie teweeg in het bedrijfsleven, verhoogt de productiviteit en biedt nieuwe mogelijkheden voor het menselijk potentieel. Op het gebied van cyberbeveiliging profiteren zowel kwaadwillenden als verdedigers van AI:

Vijandig gebruik: AI maakt geavanceerdere aanvallen mogelijk, zoals zeer overtuigende spearphishing en deepfakes.

Defensief gebruik: AI helpt verdedigers door:

- snel grote hoeveelheden beveiligingsdata te verwerken;
- bedreigingen effectiever te prioriteren;
- detectie- en responsmogelijkheden te verbeteren.

Beveiligingstools zullen echter alleen maar beter worden, waarbij beveiligingsprofessionals dankzij natuurlijke taalverwerking directer met hun systemen kunnen communiceren en systemen proactief corrigerende cyberbeveiligingsmaatregelen laat nemen.

Organisaties moeten de mogelijkheden benutten en er tegelijkertijd voor zorgen dat hun training en andere verdedigingsmechanismen up-to-date blijven. Training is de beste manier om te voorkomen dat werknemers het slachtoffer worden van geavanceerdere aanvallen.

Werken zonder wachtwoord

Wachtwoorden zijn niet langer de veiligste methoden voor identiteits- en toegangsbeheer.

Traditionele, op wachtwoorden gebaseerde systemen vertonen aanzienlijke kwetsbaarheden, waardoor ze steeds minder geschikt zijn voor de moderne behoeften op het gebied van cyberbeveiliging. Wachtwoorden zijn gevoelig voor aanvallen zoals credential stuffing, phishing en brute-force-aanvallen, waardoor organisaties vaak worden blootgesteld aan onnodige risico's. Bovendien vormt slecht gebruikersgedrag, zoals wachtwoorden opnieuw gebruiken en zwakke wachtwoorden, een extra kwetsbaarheid.

Verificatiemethoden zonder wachtwoord, zoals biometrische data, certificaten en hardwaretokens, bieden een sterker, veiliger alternatief door hele klassen wachtwoordgerelateerde bedreigingen te elimineren. De overstap naar systemen zonder wachtwoord is een cruciale evolutie in identiteits- en toegangsbeheer, waarbij beveiligingsmaatregelen worden afgestemd op de toenemende complexiteit van cyberdreigingen.

Het gebruik van technologieën zonder wachtwoord biedt ook tal van voordelen, waaronder het verkleinen van het aanvalsoppervlak, het verbeteren van de gebruikerservaring door sneller en probleemloos aan te melden en het verlagen van de IT-kosten door het verminderen van wachtwoordgerelateerde incidenten. Het gebruik van geavanceerde methoden zorgt voor een sterkere beveiligingsmentaliteit en helpt organisaties te voldoen aan wettelijke normen. De overstap naar systemen zonder wachtwoord is niet alleen een trend, het is een noodzakelijke stap om te bouwen aan een veiliger, efficiënter digitaal ecosysteem voor individuen en organisaties.

Conclusie

Cyberbeveiliging gaat een transformerend tijdperk in, dat wordt gevormd door kwantumcomputing, veranderende regelgeving en steeds geavanceerdere bedreigingen. Om voorop te blijven lopen, moeten organisaties zich openstellen voor innovaties zoals post-kwantumcryptografie, AI-gestuurde verdediging en verificatie zonder wachtwoord. Door prioriteit te geven aan paraatheid, samenwerking en strategische investeringen, kunnen bedrijven een veiligere en veerkrachtigere digitale omgeving creëren. Dit is het moment om actie te ondernemen.

Dell producten en oplossingen die kunnen helpen

Aanbevolen Dell oplossing	Omschrijving
Cybersecurity Advisory Services	Deskundige begeleiding die u kan helpen bij het plannen voor het veranderende dreigingslandschap, inclusief huidige en opkomende bedreigingen.
vCISO	Virtual Chief Information Security Officer en cyberbeveiligingsexpert die kan helpen bij het identificeren en beheren van risico's en het begeleiden van strategische besluitvorming.

Ontdek hoe u enkele van de grootste uitdagingen op het gebied van cyberbeveiliging van vandaag kunt aanpakken op **dell.com/cybersecuritymonth**